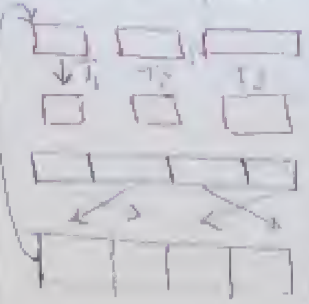
29/3/2017 الدكتور ريم الرباط محاضرة [4]

Crypto	Block Cipher (Symmetric Key 	$K_s[m(i) \oplus r(i)] = C_i$ $C_i, r(i)$ CBC mode	$C_1 = K_s[m_1 + r_1]$ $[C_1, r_1]$ $C_2 = K_s[m_2 \oplus C_1]$ $[C_2]$ $C_3 = K_s[m_3 \oplus C_2]$ $[C_3]$
Network	DES 56 bit	AES 128 bit	

* لتصفيها بـ Public/Private Encryption ⟸ Authentication و privacy بيسمح بـ

* الـ RSA Algorithm مطلوب

* Hashing الـ

* الـ Authentication من خلال الـ Hashing بنسميه Digital Signature

~~* الباقي من الربع - رابع الـ شابتر~~

Securing e-mail Slide 8.56, 5.58 --- All of it!

Securing TCP connection --- All of it!

الربع الـ PGP من الـ .pdf بترقيم الـ 736 صفحة